

1/3/1

DIALOG(R)File 351:Derwent WPI

(c) 2005 Thomson Derwent. All rts. reserv.

015258456 \*\*Image available\*\*

WPI Acc No: 2003-319385/ 200331

XRPX Acc No: N03-254626

Domain name system server data alteration system, has certificate server  
that deletes information related to computer from DNS server, after  
internet connection is disconnected

Patent Assignee: IV NETWORK KK (IVNE-N); NTT SOFTWARE KK (NITE )

Number of Countries: 001 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 2003018183	A	20030117	JP 2001199606	A	20010629	200331 B
JP 3613392	B2	20050126	JP 2001199606	A	20010629	200510

Priority Applications (No Type Date): JP 2001199606 A 20010629

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2003018183	A		7	H04L-012/56	
JP 3613392	B2		9	H04L-012/56	Previous Publ. patent JP 2003018183

BEST AVAILABLE COPY

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-018183

(43)Date of publication of application : 17.01.2003

(51)Int.Cl.

H04L 12/56

(21)Application number : 2001-199606

(71)Applicant : IVYNETWORK CO LTD  
NTT SOFTWARE CORP

(22)Date of filing : 29.06.2001

(72)Inventor : MORIZAKI MASATO  
MIZUNUMA SHINJI  
SHINODA AKIRA

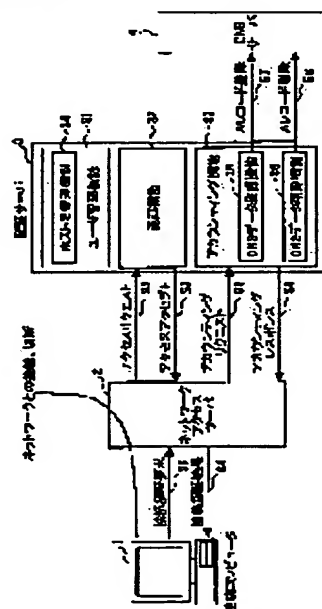
## (54) DNS SEVER DATA CHANGING SYSTEM AND AUTHENTICATION SERVER

## (57)Abstract:

PROBLEM TO BE SOLVED: To surely register/delete data in a dynamic DNS server, at using of an emergency connection service to the Internet.

SOLUTION: An authentication sever checks prescribed information in a message related with charging received from a network access server, and when the prescribed information indicates that a user computer is starting its connection to the Internet, registers data related with the computer in a DNS server; and when the prescribed information indicates that the user computer has ended the connection to the Internet, the server deletes the data related with the computer from the DNS server.

本発明の実施例におけるインターネット接続システムの構成を示す図



## LEGAL STATUS

[Date of request for examination]

29.06.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3613392

[Date of registration]

05.11.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-18183

(P2003-18183A)

(43) 公開日 平成15年1月17日 (2003.1.17)

(51) Int.Cl.<sup>7</sup>

H 0 4 L 12/56

識別記号

F I

H 0 4 L 12/56

データベース (参考)

B 5 K 0 3 0

審査請求 有 請求項の数 5 O L (全 7 頁)

(21) 出願番号 特願2001-199606 (P2001-199606)

(22) 出願日 平成13年6月29日 (2001.6.29)

(71) 出願人 500056633

株式会社アイヴィネットワーク

神奈川県横浜市中区南浅間町14-4

(71) 出願人 000102717

エヌ・ティ・ティ・ソフトウェア株式会社

神奈川県横浜市中区山下町223番1

(72) 発明者 森▲崎▼ 正人

神奈川県横浜市中区南浅間町14-4 株式

会社アイヴィネットワーク内

(74) 代理人 100070150

弁理士 伊東 忠彦

最終頁に続く

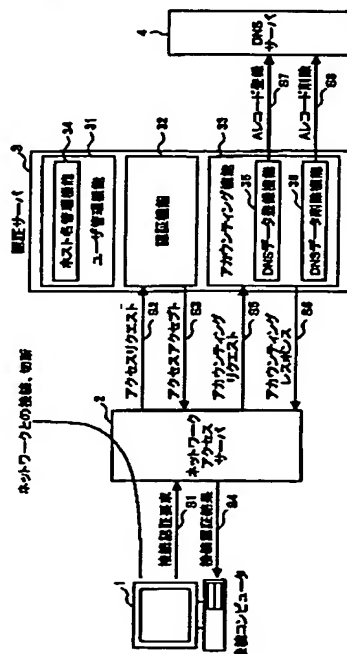
(54) 【発明の名称】 DNSサーバデータ変更システム及び認証サーバ

(57) 【要約】

【課題】 インターネットへの非常時接続サービスを利用する場合において、ダイナミックDNSサーバへのデータ登録/削除を確実にこなう。

【解決手段】 認証サーバが、ネットワークアクセスサーバから受信した課金に関するメッセージの中の所定の情報を調べ、該所定の情報が、ユーザコンピュータがインターネットへの接続を開始する旨を表す場合にはDNSサーバに前記コンピュータに関するデータを登録し、該所定の情報が、ユーザコンピュータがインターネットと接続終了した旨を表す場合にはDNSサーバから前記コンピュータに関するデータを削除する。

本発明の実施例におけるインターネット接続システムの構成を示す図



## 【特許請求の範囲】

【請求項1】 コンピュータがインターネットと接続又は切断する際にDNSサーバのデータを変更するシステムであって、

前記コンピュータからインターネット接続のための接続要求を受け付けるネットワークアクセスサーバと、  
該接続要求を受け付けたネットワークアクセスサーバからの要求に応じて前記コンピュータの認証を行う認証サーバとを有し、

認証サーバは、ネットワークアクセスサーバから受信した課金に関するメッセージの中の所定の情報を調べ、  
該所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合にはDNSサーバに前記コンピュータに関するデータを登録し、該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合にはDNSサーバから前記コンピュータに関するデータを削除することを特徴とするシステム。

【請求項2】 前記認証サーバは、

前記所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合に、前記メッセージから前記コンピュータのユーザ名とIPアドレス情報とを取得し、該ユーザ名に対応したホスト名を取得し、該IPアドレス情報と該ホスト名とを前記DNSサーバに登録し、

該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合に、前記メッセージから前記コンピュータのユーザ名を取得し、該ユーザ名に対応したホスト名を取得し、該ホスト名に対応するデータを前記DNSサーバから削除する請求項1に記載のシステム。

【請求項3】 前記課金に関するメッセージは、Radiusプロトコルにおけるアカウントングリクエストメッセージであり、前記所定の情報はアカウントングリクエストメッセージの中のステータスタイプである請求項1又は2に記載のシステム。

【請求項4】 コンピュータがインターネットと接続又は切断する際にDNSサーバのデータを変更するシステムにおいてコンピュータの認証を行う認証サーバであって、

ネットワークアクセスサーバから受信した課金に関するメッセージの中の所定の情報を調べる手段と、

該所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合にはDNSサーバに前記コンピュータに関するデータを登録する手段と、  
該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合にはDNSサーバから前記コンピュータに関するデータを削除する手段とを有することを特徴とする認証サーバ。

【請求項5】 前記登録する手段は、

前記所定の情報が、前記コンピュータがインターネット

への接続を開始する旨を表す場合に、前記メッセージから前記コンピュータのユーザ名とIPアドレス情報とを取得し、該ユーザ名に対応したホスト名を取得し、該IPアドレス情報と該ホスト名とを前記DNSサーバに登録する手段を有し、

前記削除する手段は、

該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合に、前記メッセージから前記コンピュータのユーザ名を取得し、該ユーザ名に対応したホスト名を取得し、該ホスト名に対応するデータを前記DNSサーバから削除する手段を有する請求項4に記載の認証サーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネット上のドメインネームシステム（DNS）のデータを変更する技術に関する。

【0002】

【従来の技術】インターネット上で情報発信を行う場合、コンピュータを情報発信サーバとして設置し、外部からのアクセス用のアドレスとしてIPアドレスそのものではなくURLを公開する。このURLは、ホスト名とドメイン名とサーバ上のファイルの位置から構成される。

【0003】従って、サーバにアクセスする際には、ホスト名とドメイン名の組み合わせからIPアドレスを取得する必要がある。そのために、ホスト名とドメイン名の組み合わせをIPアドレスに変換するサービスとしてドメインネームシステム（DNS）があり、RFC1035で規定されている。

【0004】すなわち、公開されたURLにより情報発信サーバへのアクセスを行う場合、ホスト名とドメイン名の組み合わせをDNSに問い合わせるIPアドレスに変換し、変換されたIPアドレスにより情報発信サーバへ接続することとなる。

【0005】さて、情報発信サーバをインターネットに接続する場合、インターネットサービスプロバイダー（ISP）の常時接続サービスを用いる方法のほか、ダイヤルアップ相当の非常時接続サービスを用いる方法がある。常時接続サービスではIPアドレスが情報発信サーバに固定的に付与されるが、ダイヤルアップ相当の非常時接続サービスではインターネットに接続する都度付与されるIPアドレスが変更される。

【0006】従って、ダイヤルアップ相当の非常時接続サービスを使用して情報発信サーバを設置した場合、ISPから付与されるIPアドレスが変更される度、すなわち、情報発信サーバがインターネットに接続する度に、DNSサーバにおけるホスト名とドメイン名との組み合わせとIPアドレスの射影を変更する必要が生じる。

【0007】従来技術では、ホストの追加、変更等があった場合のDNSサーバのデータ更新は、データファイルを手動で直接編集し更新するか、RFC2136で規定されているDNSのデータに対する動的変更方法によりDNSサーバ（ダイナミックDNSサーバ）へアクセスするツールを用いて手動で行なっている。

【0008】RFC2136で規定されている方法によりDNSデータのAレコード更新を行なう場合、ユーザが手動で接続時にDNSデータの登録、切断前にDNSデータの削除を行なうことになる。この場合、接続時は外部からのアクセスを確保するため登録を行なうが、データ削除は、接続コンピュータの不意な停止、接続回線の不意な切断、もしくは削除忘れなどにより、必ずしも行なわれるとは限らない。

【0009】

【発明が解決しようとする課題】上述したように、非常時接続サービスを利用する場合におけるDNSサーバに対するデータの登録／削除を手動で行わなければならない上、削除が確実に行なわれないという問題がある。

【0010】本発明は、上記に鑑みてなされたもので、インターネットへの非常時接続サービスを利用する場合において、DNSサーバへのデータ登録／削除を自動的に確実に行なうことを可能にする技術を提供することを目的とする。

【0011】

【課題を解決するための手段】上記目的を達成するため、本発明は次のように構成することができる。

【0012】請求項1に記載の発明は、コンピュータがインターネットと接続又は切断する際にDNSサーバのデータを変更するシステムであって、前記コンピュータからインターネット接続のための接続要求を受け付けるネットワークアクセスサーバと、該接続要求を受け付けたネットワークアクセスサーバからの要求に応じて前記コンピュータの認証を行う認証サーバとを有し、認証サーバは、ネットワークアクセスサーバから受信した課金に関するメッセージの中の所定の情報を調べ、該所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合にはDNSサーバに前記コンピュータに関するデータを登録し、該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合にはDNSサーバから前記コンピュータに関するデータを削除する。

【0013】請求項2に記載の発明は、請求項1の記載において、前記認証サーバは、前記所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合に、前記メッセージから前記コンピュータのユーザ名とIPアドレス情報とを取得し、該ユーザ名に対応したホスト名を取得し、該IPアドレス情報と該ホスト名とを前記DNSサーバに登録し、該所定の情報が、前記コンピュータがインターネットと接続終了した旨を

表す場合に、前記メッセージから前記コンピュータのユーザ名を取得し、該ユーザ名に対応したホスト名を取得し、該ホスト名に対応するデータを前記DNSサーバから削除する。

【0014】請求項3に記載の発明は、請求項1又は2の記載において、前記課金に関するメッセージは、Radiusプロトコルにおけるアカウントングリクエストメッセージであり、前記所定の情報はアカウントングリクエストメッセージの中のステータスタ입であるとする。

【0015】請求項4、5に記載の発明は、上記システムでの使用に適した認証サーバである。

【0016】本発明によれば、認証サーバが、ネットワークアクセスサーバから受信した課金に関するメッセージの種別に応じてDNSサーバのデータ登録／削除処理をすることにより、ユーザコンピュータの通信の接続／切断とDNSサーバのデータ登録／削除処理を連動させることが可能となる。従って、従来のような手動によるDNSデータ登録を行う必要がなくなり、また、DNSサーバのデータ削除を確実に行うことが可能となる。

【0017】

【発明の実施の形態】以下、図面を用いて本発明の実施例を説明する。

【0018】図1は、本発明の実施例におけるインターネット接続システムの構成を示す図である。

【0019】同図に示すインターネット接続システムは、接続コンピュータ1、ネットワークアクセスサーバ2、認証サーバ3、DNSサーバ4を有する。

【0020】接続コンピュータ1は、インターネットサービスプロバイダの非常時接続サービスを利用してインターネットに接続する情報公開サーバ等であり、ネットワークアクセスサーバ2へ接続し、認証サーバ3による認証後にネットワークアクセスサーバ2を介してインターネットへアクセス可能となる。ネットワークアクセスサーバ2は、認証及びアカウントングのためにRadiusプロトコルによって認証サーバ3へアクセスする。DNSサーバ4は、ホスト名とドメイン名の組み合わせをIPアドレスに変換する機能を有する。

【0021】認証サーバ3は、ユーザ管理機能31、認証機能32、アカウントング機能33を有し、本発明ではDNSサーバ4のデータ更新を行う機能も有する。ユーザ管理機能31は、ユーザ名、パスワードなどのユーザ情報を管理する機能であり、本発明ではホスト名管理機能34を加えて、ユーザ毎に接続するコンピュータに対するホスト名を管理する。認証機能32は、認証要求を受信した場合、ユーザ管理機能31から該当するユーザの情報を取得し、認証を行なう機能である。アカウントング機能33は、アカウントングメッセージを受信した場合にアカウントング情報をログに書き出す機能である。

【0022】本発明では、アカウントینگ機能33にDNSデータ登録機能35とDNSデータ削除機能36を追加し、DNSサーバ4のデータに対して操作を行なう。

【0023】なお、認証サーバ3で用いられるRadiusプロトコルは、インターネット接続時のユーザアクセス認証、アカウントینگ等によく用いられているものであり、認証に関するものはRFC2865、アカウントینگに関するものはRFC2866で規定されている。

【0024】上記の各サーバは、CPU、メモリ、ハードディスク、入出力装置、通信制御装置等を有するコンピュータに各サーバの処理手順を実行するためのプログラムを搭載することによって実現できる。

【0025】次に、図1を参照して、本実施例におけるインターネット接続システムの動作について説明する。なお、DNSサーバのデータ変更を除き、以下の手順はRadiusプロトコルに基づく手順である。

【0026】接続コンピュータ1からインターネット接続しようとする場合、接続コンピュータ1からネットワークアクセスサーバ2へ接続認証要求を出す(ステップ1)。その要求を受けたネットワークアクセスサーバ2は、認証のために認証サーバ3へRadiusプロトコルにより通信を行なう。すなわち、アクセスリクエストメッセージを認証サーバ3に送信する(ステップ2)。認証サーバ3により認証がなされたときには、認証サーバ3はアクセスアセプトメッセージをネットワークサーバ2に送信する(ステップ3)。これにより、接続認証結果が接続コンピュータ1に送られ(ステップ4)、接続コンピュータ1はインターネットに接続できることとなる。

【0027】また、認証が成功した場合、ネットワークアクセスサーバ2は、アカウントینگを行うためのアカウントینگリクエストメッセージを認証サーバ3へ送信し(ステップ5)、認証サーバ3はアカウントングレスポンスメッセージを返す(ステップ6)。

【0028】インターネットへの接続時のアカウントングリクエストメッセージにより認証サーバ3に通信開始であることが記録される。また、接続コンピュータ1とネットワークアクセスサーバ2間の通信が、通信終了も含めなんらかの理由のために切断された場合、ネットワークアクセスサーバ2から認証サーバ3へ通信終了を知らせるためのアカウントングリクエストメッセージが送信され、これにより認証サーバ3に通信終了であることが記録される。

【0029】本発明では、上記のアカウントングリクエストメッセージを契機として認証サーバ3がDNSサーバ4のデータ(Aレコード)の登録や削除を行う(ステップ7、8)。この動作について図2の手順に従って詳細に説明する。

【0030】図2はアカウントینگ機能の処理シーケンスを示したものであり、点線内の部分が本発明におけるDNSデータ登録機能35及びDNSデータ削除機能36の動作である。

【0031】まず、認証サーバ3がアカウントングリクエストメッセージを受信すると、アカウントングリクエストメッセージ内のステータスタイプをチェックする(ステップ11)。

【0032】図3にアカウントングメッセージのフォーマットを示す。同図における属性の部分にステータスタイプが含まれる。また、コード(4又は5)によってアカウントングリクエストかアカウントングレスポンスかが識別される。

【0033】アカウントングリクエストメッセージ内のステータスタイプは、接続コンピュータ1がネットワークアクセスサーバ2に接続される場合には、スタート(Acct-Status-type=Start)となり、接続コンピュータ1がネットワークアクセスサーバ2から切断された場合には、ステータスタイプがストップ(Acct-Status-type=Stop)となる。図4にログファイルとして出力する属性の一例を示す(接続時の例)。

【0034】次に、認証サーバ3は、上記のステータスタイプによって処理を振り分ける(図2のステップ12)。

【0035】ステータスタイプがスタートの場合には、アカウントングリクエストメッセージからユーザ名とIPアドレス情報を取得し(ステップ13)、ユーザ管理機能31のホスト名管理機能34からユーザ名に対応したホスト名を取得し(ステップ14)、そのIPアドレス情報とホスト名をAレコードとして、DNSサーバ4に登録する(ステップ15)。

【0036】ステータスタイプがストップの場合には、アカウントングリクエストメッセージからユーザ名を取得し、ユーザ管理機能31のホスト名管理機能34からユーザ名に対応したホスト名を取得し(ステップ16)、該ホスト名に対応するAレコードを、DNSサーバ4から削除する(ステップ17)。

【0037】図5(a)に、通常のユーザ管理機能でのデータ構造を示し、図5(b)に、本発明においてホスト名管理機能34を追加するために上記データ構造に“ホスト名”を加えたユーザ管理機能31のデータ構造を示す。このホスト名管理機能34を用いることにより、図6(a)に示すAレコード登録時に用いるデータ及び図6(b)に示すAレコード削除時に用いるデータを得ることが可能となる。

【0038】図7にDNSサーバ4におけるデータの記述例を示す。本発明によって、同図に示すホスト名を持つコンピュータがインターネットに接続されるときに当該ホスト名に対応するレコードが自動的に追加され、切断されるときに当該ホスト名に対応するレコードが自動

的に削除される。

【0039】続いて、アカウントログの書き込みを行い（ステップ18）、アカウントレスポンスメッセージをネットワークアクセスサーバに送信する（ステップ19）。

【0040】本発明は、上記の実施例に限定されなく、特許請求の範囲内で種々変更・応用が可能である。例えば、上記の実施例ではRadiusプロトコルを使用した場合を示したが、上記のアカウントメッセージに相当するメッセージを用いるプロトコルであれば、Radiusプロトコル以外のプロトコルにも本発明を適用することが可能である。

【0041】

【発明の効果】以上説明したように、本発明によれば、Radiusプロトコルを使用した認証サーバが、アカウントリクエストメッセージのステータスタイプに従って、DNSサーバへのデータ登録/削除を行なうこととしたので、ユーザがコンピュータをインターネット接続/切断する際に手動でダイナミックDNSサーバへデータを登録/削除する必要がなくなる。従って、インターネットサービスプロバイダは、利便性の高いインターネット非常時接続サービスを提供することが可能となる。

【0042】また、ネットワークアクセスサーバからの回線接続状態に従ったダイナミックDNSとの連動が可能となるため、接続回線の不意な切断や、接続したコンピュータの不意なダウンなどの場合も、回線切断状態として検知でき、DNSサーバに対して自動的にデータ削除処理を行なうことができ、不用意に使用しないデータ

【図3】

アカウントメッセージのフォーマットを示す図

コード	クライアント識別記号	メッセージデータ長
認証用情報		
属性(アカウント用データ)...		

【図5】

ユーザ管理機能におけるデータ構造を示す図

(a)	ユーザ名	パスワード	有効期限
-----	------	-------	------

(b)	ユーザ名	パスワード	ホスト名	有効期限
-----	------	-------	------	------

が残存することを防止することが可能となる。

【0043】

【図面の簡単な説明】

【図1】本発明の実施例におけるインターネット接続システムの構成を示す図である。

【図2】本発明の実施例におけるインターネット接続システムの動作を示すフローチャートである。

【図3】アカウントメッセージのフォーマットを示す図である。

10 【図4】ログファイルとして出力する属性の一例を示す図である（接続時の例）。

【図5】ユーザ管理機能におけるデータ構造を示す図である。

【図6】Aレコード登録又は削除時に用いるデータを示す図である。

【図7】DNSサーバにおけるデータの記述例を示す図である。

【符号の説明】

- 1 接続コンピュータ
- 20 2 ネットワークアクセスサーバ
- 3 認証サーバ
- 4 DNSサーバ
- 31 ユーザ管理機能
- 32 認証機能
- 33 アカウント機能
- 34 ホスト名管理機能
- 35 DNSデータ登録機能
- 36 DNSデータ削除機能

【図4】

ログファイルとして出力する属性の一例を示す図（接続時の例）

```

Mon Oct 4 11:54:14 1999
User-Name = "user01@xxx.co.jp#000"
NAS-IP-Address = 157.X.XX.XX
NAS-Port = 2048
NAS-Port-Type = Sync
Acct-Status-Type = Start
Acct-Delay-Time = 0
Acct-Session-Id = "307488698#000"
Acct-Authentic = RADIUS
Ascend-Modem-PortNo = 2
Ascend-Modem-SlotNo = 2
Ascend-Modem-ShelfNo = 1
Timestamp = 939005654

```

【図6】

Aレコード登録又は削除時に用いるデータを示す図

Aレコード登録時のデータ

(a) ホスト名 IPアドレス

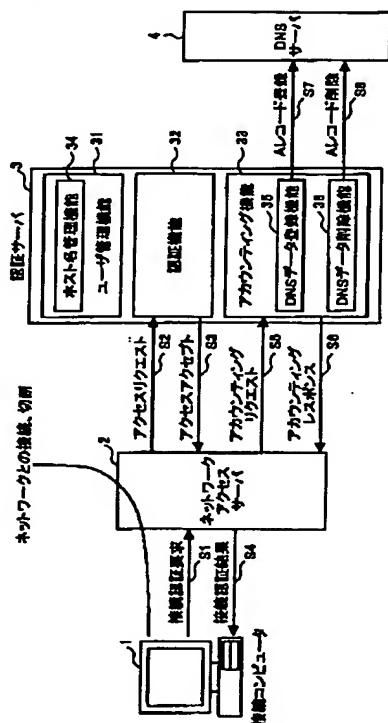
Aレコード削除時のデータ

(b) ホスト名



【図 1】

本発明の実施例におけるインターネット接続システムの構成を示す図



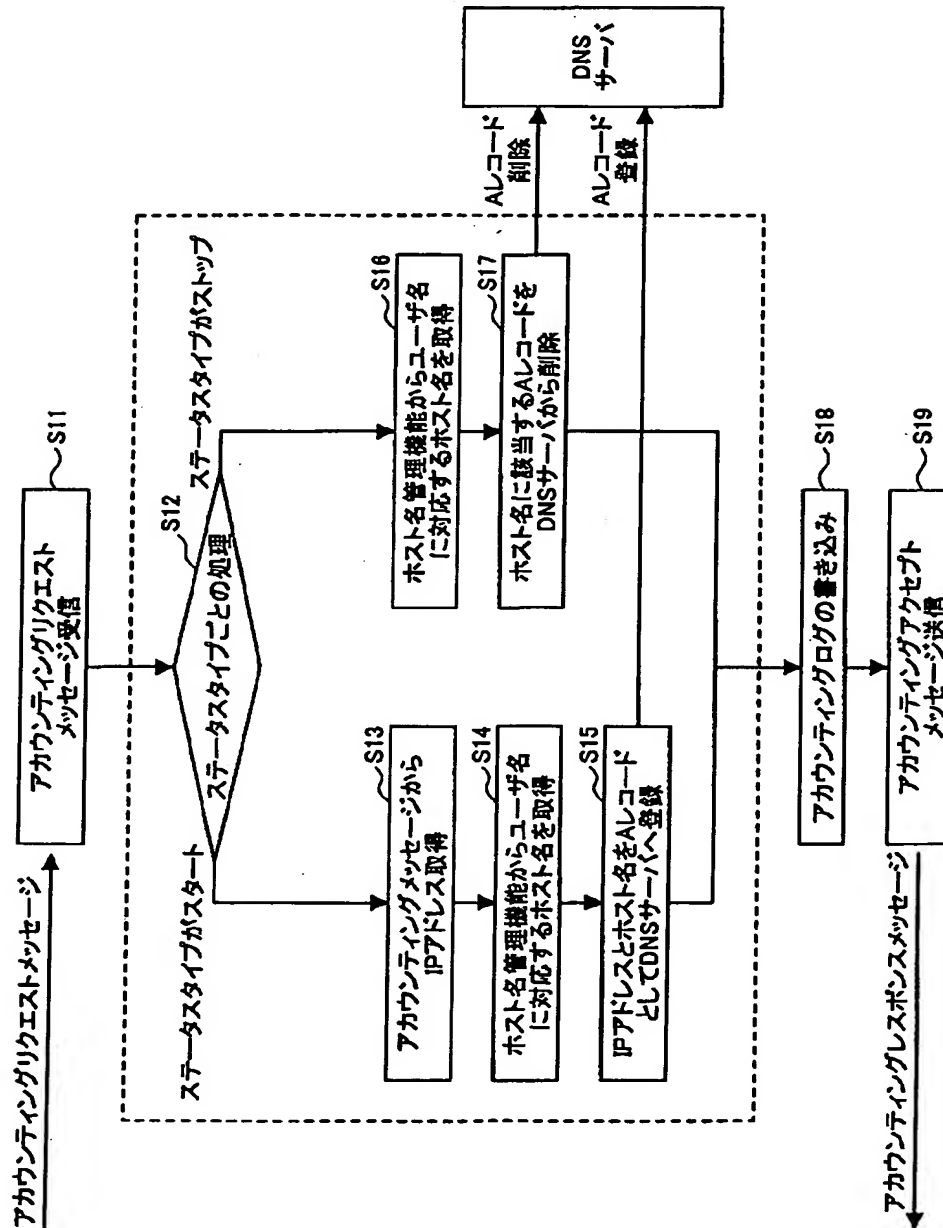
【図 7】

DNSサーバにおけるデータ記述例を示す図

ホスト名			IPアドレス
↓			↓
yellow	IN	A	192. XXX. XXX. XXX
sonic	IN	A	192. XXX. XXX. XXX
hurricane	IN	A	192. XXX. XXX. XXX

【図2】

本発明の実施例におけるインターネット接続システムの動作を示すフローチャート



フロントページの続き

(72)発明者 水沼 信治  
神奈川県横浜市西区南浅間町14-4 株式  
会社アイヴィネットワーク内

(72)発明者 篠田 晃  
神奈川県横浜市中区山下町223番1 エ  
ヌ・ティ・ティ・ソフトウェア株式会社内  
Fターム(参考) 5K030 GA15 HB08 KA05